

DOCKET NO.: 13608ROUS02U

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Donald R. HORNE

PROCESSED BY  
PG PUB DIVISION

SERIAL NO: 09/996,671

ART UNIT: 2182

NOV 27 2002

FILED: November 30, 2001

EXAMINER: Unknown

SUBJECT: MANAGEMENT OF LOG ARCHIVAL AND REPORTING FOR DATA  
NETWORK SECURITY SYSTEMS

ATTENTION: Jon Lachel - Pre-Grant Publications Division

# 7

THE ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231, U.S.A.

Sir:

**REQUEST FOR CORRECTED APPLICATION PUBLICATION**

This request is filed in respect of the above-referenced application to correct material errors in **Application Publication No. US-2002-0138762-A1** dated September 26, 2002.

Upon review we noted that between paragraph [0133] and [0134] of the published application, a section of the application from page 22, line 5 to page 41, line 30 of the original application is entirely missing. Copies of the missing pages of the application as filed are transmitted herewith.

The Commissioner is hereby authorized to charge any fees which may be required, or credit and overpayment to **Deposit Account No. 14-1315**.

Yours very truly,

Donald R. HORNE

By Angela C. de Wilton,  
Patent Agent  
Registration. No. 35,763ACdW/jo:Encis.  
c/o NORTEL NETWORKS LIMITED  
Intellectual Property Law Group  
P.O. Box 3511, Station "C"  
Ottawa, Ontario, Canada K1Y 4H7Phone: (613) 768-3020  
FAX: (613) 768-3017

Date: November 27, 2002

### Components Inputs and Outputs

This section provides further details of the component inputs and outputs used in the system according to the embodiment.

5

#### Log Collector (LC)

Input from LCM:

System\_configuration

Retrieval\_Interval={default=24 hrs | hourly  
10 interval=1 - 24 hrs}  
Cleanup\_Interval={ default=7 days | weekly  
interval=1 - 7days)

Output to LCM:

15 Log transfer list  
LC\_Name {FQHN, IP address}  
SD\_Name {FQHN, IP address}  
Date  
Retrieval\_Interval  
20 Time  
Files={file1, file2, file3...}  
Errors  
file 1  
file 2  
25 file 3

#### Log Collector Manager (LCM)

Input from DAM:

System\_configuration

30 Retrieval\_Interval={default=24 hrs | hourly  
interval=1 - 24 hrs}  
Cleanup\_Interval={ default=7 days | weekly  
interval=1 - 7days)

LC\_List={LC\_Name1, LC\_Name2, LC\_Name3...}

```
LC_Name 'n'={FQHN, IP address}
SD_List={SD_Name1, SD_Name 2, SD_Name
3...)

SD_Name 'n'={FQHN, IP address}
5 LCM_status_request /* request status update of LC
log archiving managed by LCM */

Input from LC:
Log transfer list
10 LC_Name {FQHN, IP address}
SD_Name {FQHN, IP address}
Date
Retrieval_Interval
Time
15 Files={file1, file2, file3...)
Errors
file 1
file 2
file 3
20

Output to SM:
Log transfer list
LCM_Name {FQHN, IP address}
LC_Name {FQHN, IP address}
25 SD_Name {FQHN, IP address}
Date
Retrieval_Interval
Time
Files={file1, file2, file3...)
30 file 1
file 2
file 3
```

Output to DAM:

```
Log archival transaction complete
    LCM_Name {FQHN, IP address}
    LC_Name {FQHN, IP address}
    SD_Name {FQHN, IP address}
5      Errors
    LCM_archival_complete /*when all logs have been
transferred to the SM for that interval*/
    LCM_status_update
        LC_List={LC_Name1, LC_Name2, LC_Name3...}
10      LC_Name'n'={FQHN, IP address,
status=[archived | cached |waiting]}
```

**Storage Manager (SM)**

Input from LCM:

```
15      Log transfer list
        LCM_Name {FQHN, IP address}
        LC_Name {FQHN, IP address}
        SD_Name {FQHN, IP address}
        Date
20      Retrieval_Interval
        Time
        Files={file1, file2, file3...}
        file 1
        file 2
25      file 3
```

Input from DAM:

```
    System_configuration
        Archival_Duration={type1, type2, type3...}
30      type'n'={online=[number_months],
offline=[number_months]}
    Log_Location_Request
        SD_Type
        SD_Name {FQHN}
```

```

    Date
    ONLINE-OFFLINE_bit /* bit 'on' when auto
analysis is being done on newly arrived logs */
    Filepath_List={filepath1, filepath2,
5  filepath3...} /* file path given for restored offline
logs */
    Log_Info_Request
        SD_Type
        SD_Name {FQHN}
10    Date
    Online_Table_Request
    Offline_Table_Request

Output to DAM:
15    Log_Location_Reply
        SD_Type /* type derived from name */
        SD_Name {FQHN, IP address}
        Date
        Retrieval_Interval
20    Time
        File_Location_List={filepath1, filepath2,
filepath3...}
        filepath'n'={ONLINE_bit, ONLINE=filepath}
    Log_Info_Reply
25    SD_Type
        SD_Name {FQHN, IP address}
        LCM_Name
        LC_Name
        Online_Offline
30    Offline_Date
        Online_Date
        Log_Date
        Retrieval_Interval
    Online_Table_Reply
```

**Offline\_Table\_Reply****Online Log Archival Table**

SD\_Type  
5 SD\_Name  
IP\_address  
LCM\_Name  
LC\_Name  
Archival\_Date  
10 Log\_Date  
Retrieval\_Interval  
Time={time1, time2, time3...}  
Filepath={filepath1, filepath2, filepath3...}

**15 Offline Log Archival Table**

SD\_Type  
SD\_Name  
IP\_address  
LCM\_Name  
20 LC\_Name  
Offline\_Date  
Log\_Date  
Retrieval\_Interval  
Time={time 1, time2, time3}  
25 Filepath={N/A, N/A, N/A}

**Data Analysis Manager (DAM)**

Input from LCM:

30 Log archival transaction complete  
LCM\_Name {FQHN, IP address}  
LC\_Name {FQHN, IP address}  
SD\_Name {FQHN, IP address}  
Errors

```
LCM_archival_complete /*when all logs have been
transferred to the SM for that interval*/
```

```
LCM_status_update
```

```
LC_List={LC_Name1, LC_Name2, LC_Name3...}
```

```
5      LC_Name'n'={FQHN, IP address,
status={archived | cached |waiting}}
```

```
Input from WAS:
```

```
Log_Location_Request /* for custom analysis */
```

```
10      SD_Type
```

```
SD_Name {FQHN, IP address}
```

```
Date_Range={Date | From_To}
```

```
Online={ONLINE | OFFLINE}
```

```
15      Offline_File_Location_List={filepath1,
filepath2, filepath3...}/* restored filepath known */
```

```
FULL_TEXT={ON | OFF}
```

```
Custom_Metrics_Request
```

```
Filter_Type={customized filter keys}
```

```
SD_Type
```

```
20      SD_Name {FQHN}
```

```
Date_Range={Date | From_To}
```

```
Online_Table_Request
```

```
Offline_Table_Request
```

```
25 Input from SM:
```

```
Log_Location_Reply
```

```
SD_Type
```

```
SD_Name {FQHN, IP address}
```

```
Date
```

```
30      Retrieval_Interval
```

```
Time
```

```
File_Location_List={filepath1, filepath2,
filepath3...}
```

```
filepath'n'={ONLINE_bit, ONLINE=filepath}
```

## Log\_Info\_Reply

SD\_Type

SD\_Name {FQHN, IP address}

LCM\_Name

5 LC\_Name

Online\_Offline

Offline\_Date

Online\_Date

Log\_Date

10 Retrieval\_Interval

Online\_Table\_Reply

Offline\_Table\_Reply

## Input from DAS:

15 System\_Configuration

Archival\_Duration={type1, type2, type3...}

type'n'={online=[number\_months],

offline=[number\_months]}

Retrieval\_Interval={default=24 hrs | hourly

20 interval=1 - 24 hrs}

Cleanup\_Interval={ default=7 days | weekly

interval=1 - 7days)

SDtypes={type1, type2, type3...}

type'n'={code, description}

25 Devicelist={device1, device2, device3...}

Filters={filtertype1, filtertype2,

filtertype3...}

filtertype'n'={key1, key2, key3...}

Alarms={alarmtype1, alarmtype2, alarmtype3...}

30 alarmtype'n'={key1, key2, key3...}

LCMlist={lcm1, lcm2, lcm3...}

lcm'n'={FQHN, IPaddr, responsibility}

## Output to LCM:



## SD system configuration file:

```
Retrieval_Interval={default=24 hrs | hourly
interval=1 - 24 hrs}
```

```
Cleanup_Interval={ default=7 days | weekly
5 interval=1 - 7days)
```

```
LC_List={LC_Name1, LC_Name2, LC_Name3...}
```

```
LC_Name 'n'={FQHN, IP address}
```

```
SD_List={SD_Name1, SD_Name 2, SD_Name
3...)
```

```
10 SD_Name 'n'={FQHN, IP address}
```

```
LCM_status_request /* request status of LC log
archiving managed by LCM */
```

## Output to SM:

```
15 System_Configuration
```

```
Archival_Duration={type1, type2, type3...}
```

```
type'n'={online=[number_months],
offline=[number_months]}
```

```
Log_Location_Request
```

```
20 SD_Type
```

```
SD_Name {FQHN}
```

```
Date
```

```
ONLINE-OFFLINE_bit /* bit 'on' when auto
analysis is being done on newly arrived logs */
```

```
25 Filepath_List={filepath1, filepath2,
filepath3...}
```

```
Log_Info_Request
```

```
SD_Type
```

```
SD_Name {FQHN}
```

```
30 Date
```

```
Online_Table_Request
```

```
Offline_Table_Request
```

## Output to WAS:

```
Full_Text_Reply
    Logfile_Text_Buffer /* for read-only access */
Custom_Metrics_Reply
    Metrics_Table
5        Status
        Errors
        Alarms
        Search_Results
    Online_Table_Reply /* summary of logs archived
10 online */
    Offline_Table_Reply /* summary of logs archived
offline */

Output to DAS:
15    Session_Analysis
        Date={Month, Day, Year}
        Start_Time
        Session_ID
        Device_Type
20    Logfile_Type
        Logfile_Date_Time
        Retrieval_Interval
    Session_Results
        Date={Month, Day, Year}
25    Completion_Time
        Session_ID
        Device_Type
        Logfile_Type
        Logfile_Date_Time
30    Error_Code
        Alarms={none | [alarm1, alarm2, alarm3...]}
        Errors={none | [error1, error2, error3...]}
        Metrics={key1results, key2results,
key3results...}
```

key'n'results={hit1, hit2, hit3...}

Device\_Update

Device\_Type

Device\_Name

5 Status={ACTIVE, HISTORIC}

### Data Analysis Store (DAS)

Database Schema

TABLE: analysis\_session (used to store information about  
10 the logfile analysis)

#### FIELDS:

session\_id /\* incorporate the date into the  
sessionid \*/  
15 year /\* Required for \*/  
month /\* ease of extraction of \*/  
day /\* summary metrics.\*/  
device\_type (name of firewall contivity switch,  
spam machine,...)  
20 logfile\_type (type of file that was parsed. ie.  
some SDs will produce a number of logfiles)  
logfile\_date (date and time of logfile)  
retrieval\_interval (system log retrieval rate)  
start\_time /\* required to track DAM-system \*/  
25 completion\_time /\* performance \*/

TABLE: session\_alarms

#### FIELDS:

session\_id  
30 alarmcode  
status /\* status of each alarm - active or  
acknowledged \*/  
severity

TABLE: session\_errors

FIELDS:

session\_id  
5 errorcode  
status /\* status of each error - active or  
acknowledged \*/  
severity

TABLE: logfile\_types (used to store information about  
10 versions of software e.g., firewall - Raptor 4.0 vs  
Raptor 6.0)

FIELDS:

device\_type  
15 logfile\_type

TABLE: metric\_types (used to store information about the  
metrics that need to be calculated and where to find the  
results)

20

FIELDS:

metric\_id (this will be a number from 1 - 30  
and is the place where the results are stored in the  
tables. For example, if this has a value of 2, then in  
25 the individual results tables the result of this metric  
is stored in the metric2 field.)

device\_type (ie.  
FIREWALL, SPAM, CONTIVITY, FTPDROPBOX, USER\_STATS)

logfile\_type (e.g. Raptor 4, Raptor 6)  
30 metric\_name (this is the name that is used to  
describe the particular metric being found ie. Number of  
FTP connects)

metric\_key (this is the value that is being  
searched ie. ftp.\*connection for)

status (as we are storing all metrics for many years in the database, a particular metric that was used in the past may no longer be valid but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is ACTIVE, then it will be used for analysis)

TABLE: user\_table (used to store information about the users accessing this tool)

10

## FIELDS:

userid (ie. CN for certs or userid)

device\_type (i.e.

ALL, FIREWALL, SPAM, CONTIVITY, FTPDROPBOX, USER\_STATS)

15

type\_of\_access (e.g. DBA, ANALYST, HELPDESK,

CORP-INVESTIGATIONS)

user\_name

user\_phone

TABLE: access (used to store information about the

20 different levels of access)

## FIELDS:

type\_of\_access (e.g. DBA, ANALYST, HELPDESK,

CORP-INVESTIGATIONS)

25

TABLE: special\_access (used to determine access rights to a log in scenarios where specific, limited access is granted)

## FIELDS:

30

userid (ie. CN for certs or userid)

device\_name ( i.e. ALL, FQHN(S)) /\* required for security investigations \*/

date (i.e. ALL, DATE RANGE) /\* required for security investigations \*/

TABLE: firewall (used to store the metrics gathered on a per firewall basis per logfile basid - for the first cut there will be one entry per firewall per day but as the processing becomes more often, there may be many per  
5 firewall per day.)

## FIELDS:

session\_id

metric1 to metric 30 (used for counts and sums)

10 TABLE: firewall\_monthly (used to store firewall information but summarized by month)

## FIELDS:

firewall

15 year

month

metric1 to metric 30

TABLE: firewall\_user (used to store firewall information based on the USER\_STATS)

20

## FIELDS:

transaction\_type - things like connects per userid, bytes transferred per userid, etc. This information is done on a per firewall per logfile basis)

25 session\_id

userid

metric1 to metric 30

TABLE: firewall\_keyword (used to store the matched keyword information. This is done on a per firewall per  
30 logfile basis.)

## FIELDS:

session\_id

search\_key

matched\_line (string where the match was found)  
userid (if possible, the userid extracted from  
the matched line)

count(?) (ongoing count rather than additional  
5 entries in the db?)

TABLE: contivity (used to store the metrics gathered on a  
per contivity basis per logfile basis)

FIELDS:

10 session\_id  
metric1 to metric 30 (counts and sums)

TABLE: contivity\_monthly (used to store contivity  
information but summarized by month)

15 FIELDS:

contivity  
year  
month  
metric1 to metric 30

20 TABLE: contivity\_user (used to store contivity  
information based on the USER\_STATS)

FIELDS:

25 transaction\_type (things like connects per  
userid, bytes transferred per userid, etc. this  
information is done on a per contivity per logfile basis)

session\_id  
userid  
metric1 to metric 30

30 TABLE: contivity\_keyword (used to store the matched  
keyword information. This is done on a per contivity per  
logfile basis.)

FIELDS:

session\_id  
search\_key  
matched\_line (string where the match was found)  
userid (if possible, the userid extracted from  
5 the matched line)

count(?) (ongoing count rather than additional  
entries in the db?)

TABLE: dropbox (used to store the metrics gathered on a  
per dropbox basis per logfile basis)

10

FIELDS:

session\_id  
metric1 to metric 30

TABLE: dropbox\_monthly (used to store dropbox information  
15 but summarized by month)

FIELDS:

dropbox  
year  
20 month  
metric1 to metric 30

TABLE: dropbox\_user (used to store firewall information  
based on the USER\_STATS)

25

FIELDS:

transaction\_type - things like connects per  
userid, bytes transferred per userid, etc. this  
information is done on a per dropbox per logfile basis)

session\_id  
30 userid

metric1 to metric 30

TABLE: dropbox\_keyword (used to store the matched keyword  
information. This is done on a per firewall per logfile  
basis.)



## FIELDS:

session\_id  
keyword\_key (key that was looked for)  
5 matched\_line (string where the match was found)  
userid (if possible, the userid extracted from  
the matched line)  
count(?) (ongoing count rather than additional  
entries in the db?)  
10 TABLE: list\_contivity (used to store the list of  
contivities that have information stored in this  
database)

## FIELDS:

15 device\_status (as we are storing metrics for  
many contivities for many years in the database, a  
particular contivity that was used in the past may no  
longer be valid but still requires a  
placeholder in the database for historic data. The  
20 possible entries in this field are ACTIVE, or HISTORIC  
where if the  
status is ACTIVE, then it will be used for  
analysis)  
device\_name  
25 logfile\_type  
TABLE: list\_dropboxes (used to store the list of  
dropboxes that have information stored in this database)

## FIELDS:

30 device\_status (as we are storing metrics for  
many dropboxes for many years in the database, a  
particular dropbox that was used in the past may no  
longer be valid but still requires a  
placeholder in the database for historic data. The

possible entries in this field are ACTIVE, or HISTORIC where if the

status is ACTIVE, then it will be used for analysis)

5 device\_name  
logfile\_type

TABLE: list\_firewalls (used to store the list of firewalls that have information stored in this database)

10 FIELDS:

device\_status (as we are storing metrics for many firewalls for many years in the database, a particular firewall that was used in the past may no longer

15 be valid but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is ACTIVE, then it will be used for analysis)

device\_name  
20 logfile\_type

TABLE: list\_keywords (used to store the list of keywords that are to be used as part of an analysis)

FIELDS:

25 search\_key (search string)  
device\_type  
logfile\_type

responsibility (group who supplied the keyword and is responsible to investigate when found - HR (Human  
30 Resources), NS (Network Security), CS  
(Corporate Security))

status (as we are storing metrics for many firewalls for many years in the database, a particular firewall that was used in the past may no longer be valid

but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is ACTIVE, then it will be used for analysis)

5 TABLE: mailshield (used to store mailshield metrics)

FIELDS:

session\_id

metric1 to metric 30 (sum and counts)

10 logfile\_type

TABLE: spam\_rejections (used to store top 10 rejection types)

FIELDS:

15 session\_id

reject1 to reject10

occurrence1 to occurrence10

TABLE: list\_mailshields (used to store the list of mailshields that have information stored in this  
20 database)

FIELDS:

device\_status (as we are storing metrics for many mailshields for many years in the database, a  
25 particular mailshield that was used in the past may no

longer be valid but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the

30 status is ACTIVE, then it will be used for analysis)

device\_name

TABLE: mailshield\_monthly (used to store mailshield information but summarized by month)

## FIELDS:

mailshield

year

5 month

metric1 to metric 30

TABLE: blocked (used to store blocked metrics)

## FIELDS:

10 session\_id

recipient\_emailid

reason (store the reason that the email was  
blocked)

subject (the subject of the blocked email)

15 sender

TABLE: owners

## FIELDS:

responsibility (ie, HR (Human Resources, NS  
20 (Network Security), CS (Corporate Security))  
contact\_name (person to contact when matched)  
userid  
contact\_phone  
contact\_email (This is key so that an email can  
25 be sent out, assuming we decide to automate this  
function)

TABLE: error\_list (used to store information about  
possible system errors)

## 30 FIELDS:

errorno

severity

description

TABLE: alarm\_list (used to store information about log alarms)

FIELDS:

5           alarmcode  
            severity  
            description

TABLE: device\_types (used to store list of valid device\_types - these will be hard-coded into this table )

10

FIELDS:

            device\_type (i.e. FIREWALL, CONTIVITY, SPAM,...)

TABLE: lcm\_list (used to store list of Log Collector  
15 Managers)

FIELDS:

            device\_name  
            responsibility (string - depending on  
20 implementation could be geographic or device type dependent)

TABLE: sys\_config (used to store list of system parameters)

25

FIELDS:

            retrieval\_interval  
            cleanup\_interval  
            device\_type  
            online\_duration  
30           offline\_duration

Intellectual Property Law Group  
P.O. Box 3511, Station C  
Ottawa, Ontario, Canada  
K1Y 4H7

PROCESSED BY  
PG PUB DIVISION

NOV 27 2002

**NORTEL**  
**NETWORKS**

*How the world shares ideas.*

## Fax Cover Sheet

Date November 27, 2002

To Jon Lachel  
Pre-Grant Publications Division  
U.S. PATENT & TRADEMARK OFFICE

From Angela C. de Wilton  
Nortel IP Law Group

Fax # (703) 305-8568 Fax # 613-768-3017

Phone # (703) 605-4285- Phone # 613-768-3020

No. of Pages 21  
To Follow

Message Re: U.S. Patent Application Serial No. 09/996,671  
Docket No.: 13608ROUS02U

Please see attached Request for Corrected Application Publication.

### CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office, Fax No. 703-305-8568 on the date shown below.

  
Signature

*Nov 27, 2002*  
Date

Joanne Ohmayer (613-768-3005), Facsimile Operator for this transmission  
Nortel Networks Corporation, Intellectual Property Law Group

This facsimile transmission is intended only for the use of the individual or entity to which it is addressed and may contain information which is privileged and confidential. If the reader of this message is not the intended recipient, or the employee responsible for delivering this communication to the intended recipient, you are hereby notified that any disclosure, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone to arrange for its return. Thank you.

### Treatment of Originals:

☒ Retained on File ☐ Sent by Post ☐ Sent by Courier

For enquiries about this transmission, please call Joanne Ohmayer at (613) 768-3005 (ESN 398)